I N S T A L L A T I O N S L E I T F A D E N

Sat>IP anywhere

Dieser Leitfaden beschreibt die Installation der Windows-Server-Software und die Verbindung des Android-Clients (Handy, Tablet, Android TV, Fire TV). Die Server-App transkodiert SAT>IP oder DVB-C über IP und stellt das Programm im eigenen Netz und, mit HTTPS, auch von unterwegs bereit.

Neu	1. Beim ersten Start sind keine wiederholten Neustarts mehr nötig. Ist SSL konfiguriert, läuft Steuerung und Videostream über denselben HTTPS-Port. Der HTTP-Port bleibt für die rein lokale Nutzung (Android TV z.B.). 2. Per Transponder Scans können jetzt M3U Dateien selbst erstellt werden. 3. Der Server erkennt nun Brute-Force Angriffe.

1 Voraussetzungen

- Windows 10 oder 11, 64-bit. Ein SAT>IP-Server oder ein DVB-C-Gerät mit IP-Schnittstelle im selben LAN.
- Feste IP für das SAT>IP-Gerät, oder eine DHCP-Reservierung im Router. Die Server-App merkt sich die gefundene Adresse.
- Für den Zugriff von außen: DynDNS-Name im Router und UPnP, oder eine manuelle Portfreigabe.
- Android-App aus dem Play Store. iOS und tvOS sind noch im Beta Stadium.

2 Server installieren

Download und Readme liegen auf https://sat-ip-anywhere.com/Download.

Portable/ ZIP

- Archiv herunterladen und in einen Ordner entpacken, zum Beispiel C:\satipanywhere. Kein privilegiertes Verzeichnis nötig aber möglich. Keine Admin Rechte nötig um das Setup zu durchlaufen.
- Die EXE starten. Beim ersten Start legt die App settings.json an und führt durch die Einrichtung von UPnP, Ports und Zugangsdaten.

Microsoft Store

Die Store-Version installiert nach Programme\WegeApps\anywhere. Konfiguration und Zertifikat liegen im Benutzerprofil (AppData), nicht neben der EXE. Ein Autostart wird automatisch konfiguriert (ggf. entfernen: Start der>Einstellungen>, Apps, sat-ip-anywhere-server > aus) und gilt für das Konto, das installiert hat.

Auf wenigen Rechnern darf die App den HTTPS-Port nicht selbst binden. Dann einmal das mitgelieferte Skript run-after-first-start-for-ssl.bat ausführen und die Administratorabfrage bestätigen. Das ist die Ausnahme, nicht der normale erste Start.

3 Router vorbereiten

Automatisches Port Management per UPnP wird empfohlen. Die App öffnet dann den HTTPS oder die HTTP Stream Ports (Legacy, energiesparend für mobile Geräte) und schließt sie wieder, wenn sie beendet wird. Dazu muss zunächst im Router – hier in der Fritz!Box – dem PC erlaubt werden, Ports zu öffnen und zu schließen:

1. Experten-Ansicht aktivieren: Links auf „Ansicht: Standard“ klicken, sodass dort „Ansicht: Erweitert“ steht.

2. Heimnetz->Netzwerk->Netzwerkeinstellungen->“Statusinformationen über UPnP übertragen“ aktivieren.
3. Internet-> Freigaben->Windows PC->“Selbstständige Portfreigabe für dieses Gerät erlauben“

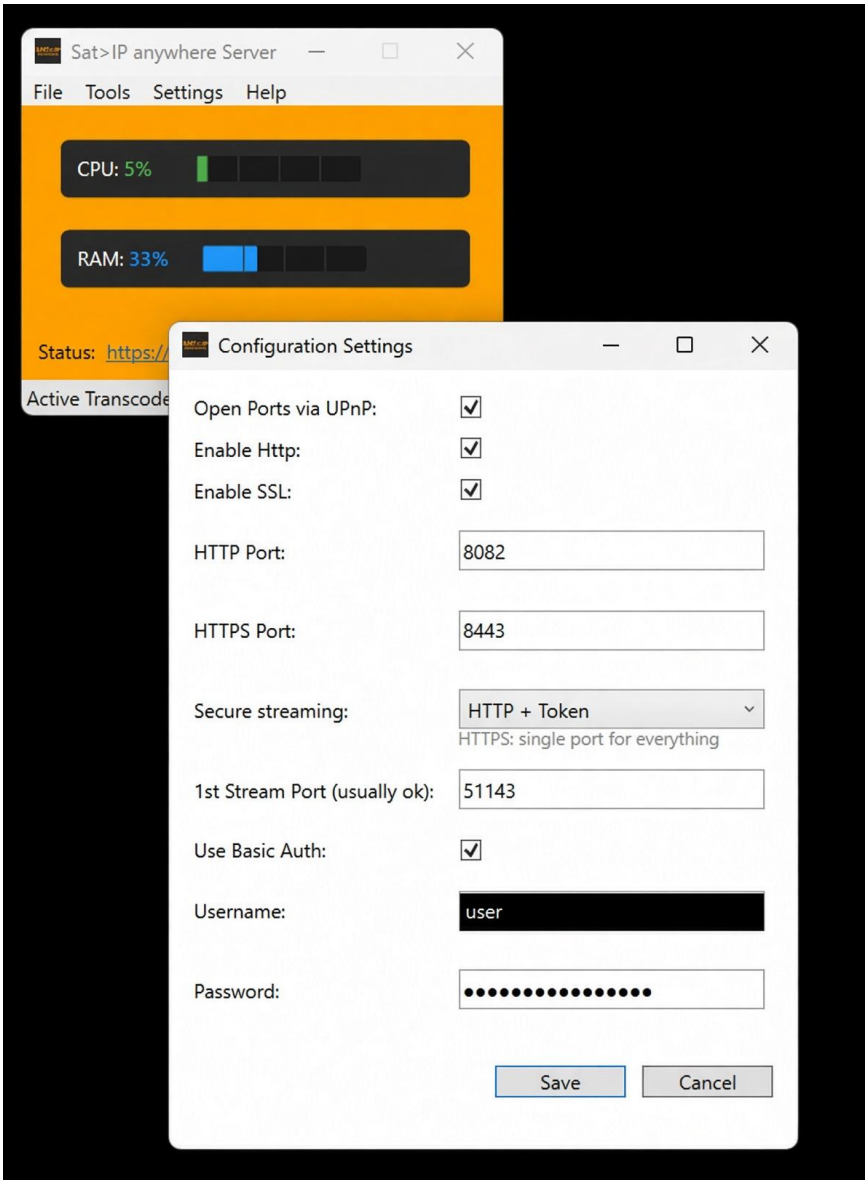
Eine ähnliche Einstellung findet sich in anderen Router ggf. unter dem Punkt UPnP. Für die Fritz!Box gibt es hier eine ausführliche Anleitung:

https://www.giga.de/hardware/fritzbox/tipps/fritzbox-upnp-aktivieren-so-gehts-richtig/

Bei anderen Routern heißt der Schalter meist nur UPnP. Eine FRITZ!Box-Anleitung steht unter giga.de, Stichwort FRITZ!Box UPnP aktivieren. Den DynDNS-Namen trägt man im Router ein, zum Beispiel über ddnss.de. Eine FRITZ!Box-Anleitung dazu steht bei heimnetz.de.

4 Ersteinrichtung

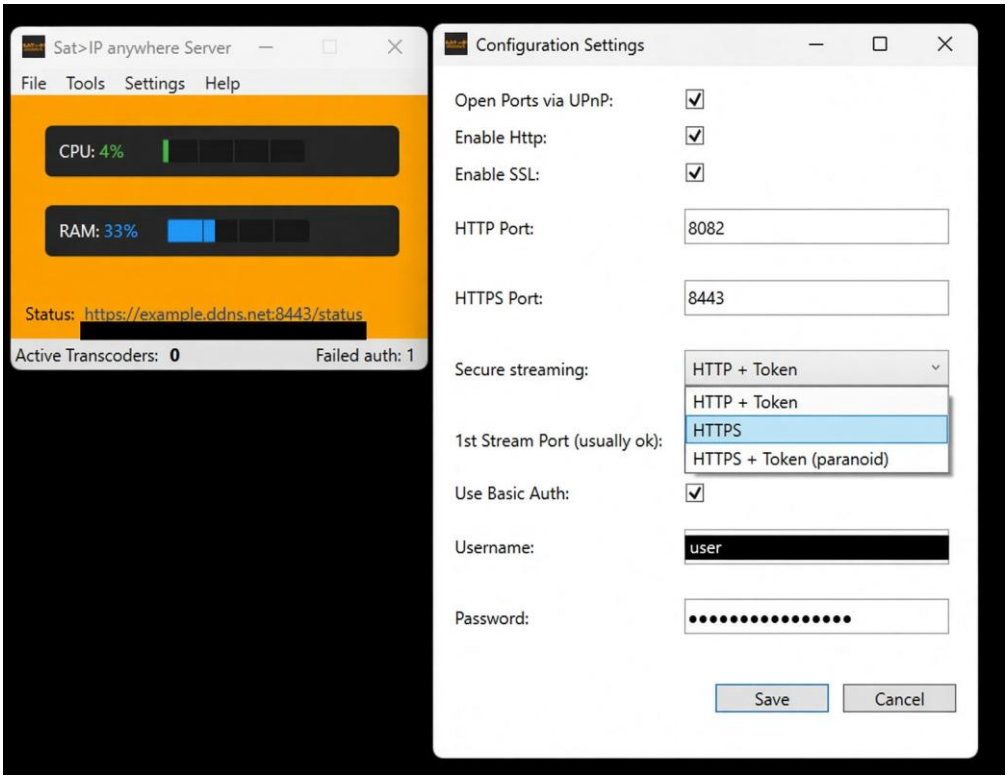
Am Anfang steht die Entscheidung ob man per VPN, Wireguard oer Tailscale auf die Server-Applikation zugreifen möchte (einfache http Konfiguration) oder per nativem HTTPS. Entscheidet man sich für HTTPS sollte ein langes und komplexes Passwort gewählt werden auch wenn der Server mittlerweile eine Brute-Force Erkennung mitbringt.



Settings: Nach dem Speichern wird die Anwendung geschlossen und muss neu gestartet werden, damit die Port(s) neu gebunden werden und ggf. ein Zertifikat erstellt werden kann.

- Open Ports via UPnP: an, wenn der Router das unterstützt.
- Enable HTTP: zum Testen, für Android TV oder VPN Nutzung. Port niemals im Router freigeben.
- Enable SSL: für unterwegs. Üblich ist 8443. Mit SSL läuft die gesamte Übertragung über diesen einen Port, Steuerung und Bild.
- 1st Stream Port: nur für den HTTP-Token-Modus relevant, üblicherweise 51111 oder höher. Von einer manuellen Freigabe im Router wird definitiv abgeraten.
- Use Basic Auth, Username und Password: in der Client-App dieselben Werte eintragen.

Secure streaming

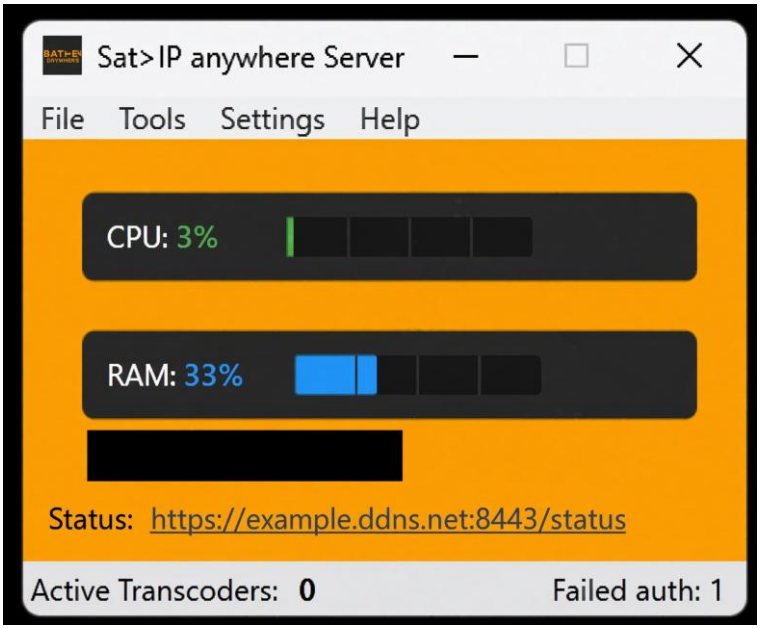


Streaming-Modus. Im Hintergrund eine Beispiel-Adresse, kein echter DynDNS-Name.

- HTTP + Token: Jede (Neu-)Verbindung holt ein neues Token (per SSL – wenn SSL konfiguriert wurde) vom Server, der das Token nach dem Verbindungsaufbau sofort verwirft. Sollte halbwegs sicher sein, aber eine Garantie dafür gibt es nicht. (*)
- HTTPS: ein Port für alles. Das ist die normale und empfohlene Konfiguration.
- HTTPS + Token (paranoid): Derselbe eine HTTPS-Port, zusätzlich ein Token pro Connect/ Reconnect. Empfohlen, wenn sich im Ausland aufhält.

Das Zertifikat erzeugt die App aus dem DynDNS-Namen und einem Zertifikatpasswort. Das Zertifikat-passwort ist nicht das Login der App und wird später nicht wieder abgefragt. Den QR-Code öffnet man hier: Settings, Network & Security, Certificate QR-Code. Er gilt für alle Geräte und ändert sich nicht, solange das Zertifikat nicht neu erstellt wird.

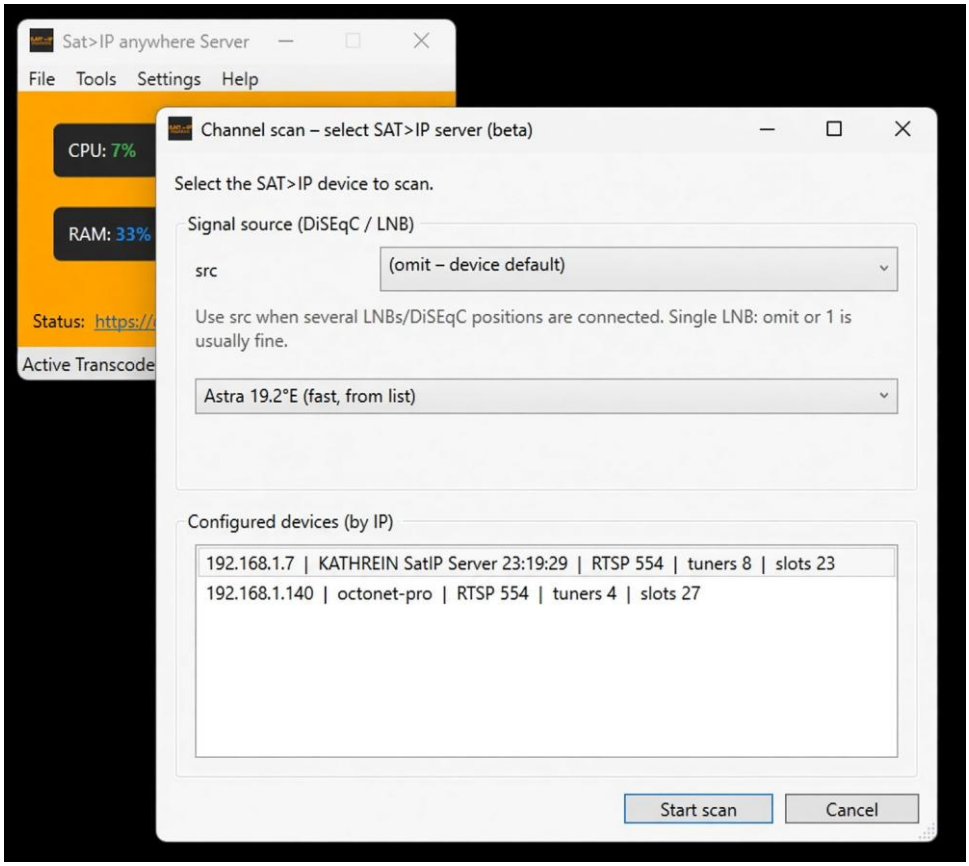
Windows fragt beim ersten Start in der Regel, ob die App durch die Firewall darf. Das zulassen. In der Statuszeile steht danach die erreichbare Adresse, zum Beispiel https://example.ddns.net:8443/status.



Hauptfenster nach dem Start. Die ddns Adresse ist ein Beispiel.

5 Kanäle

Eine fertige Senderliste liefert die App nicht direkt. Entweder eine externe M3U (z.B. https://github.com/dersnyke/satipplaylists oder aus der Fritz!Box Cable Weboberfläche) importieren (File, Import M3U Playlist) oder den eingebauten Satelliten-Scan nutzen.



Kanalscan. Ein LNB: src weglassen oder 1. Mehrere LNBs: die DiSEqC-Position setzen.

1. Gerät in der Liste wählen und Start scan. Für Astra 19,2° Ost und Türksat 42°E sind die KU-Band Frequenzen bereits hinterlegt. Daher ist der Channel Scan schneller als bei einem „blind scan“.

2. Die m3u Datei wird im Verzeichnis scan abgelegt und kann dann ggf. editiert werden, was aber normalerweise nicht nötig ist.
3. m3u Datei importierten: siehe oben
4. Tools, Channel Configuration: gewünschte Kanäle dem jeweiligen SAT>IP Server zuordnen.
5. Save List as JSON. Neustart nicht nötig.
6. Erst danach beantwortet die App Programm- und EPG-Anfragen.

Wird kein SAT>IP-Server gefunden, das SAT>IP Gerät neu starten oder das Netzwerkkabel kurz ziehen. Die IP muss danach dieselbe sein.

6 Android-App

Play Store, Sat>IP anywhere. Oben rechts Menü => Setup.

1. IP or DDNS Host: DynDNS-Name von unterwegs, oder die LAN-IP des Windows-PCs für rein lokales HTTP. Nicht die IP des SAT>IP-Geräts.
2. Client Id: eine Id pro Gerät, 1 bis x. Zwei Endgeräte brauchen zwei unterschiedliche Ids.
3. HTTPS an, wenn am Server SSL konfiguriert wurde. Der Port ist dann der HTTPS-Port, zum Beispiel 8443. Bei lokalem HTTP den HTTP-Port eintragen und https aus lassen.
4. Username und Password wie in der Server-App.
5. Scan Certificate: QR-Code vom Server scannen. Die Markierung in den Code halten. Einmal reicht.

Aufnahmen laufen über den Server und erscheinen in der App unter Recordings. Dafür sollte die Server-App aktuell sein.

1. Wenn möglich unter Menü => Playback Settings compatibility mode auf „aus“.
2. Data Saver für unterwegs, wenn die Bildqualität zweitrangig ist. (ca. 1Mbit/s)

7 Wenn etwas hakt

- Einfach in der WhatsApp Support Gruppe nachfragen. https://chat.whatsapp.com/IjLmnS03KMPH9GIZgkliE9
- Failed auth in der Statuszeile zählt fehlgeschlagene Anmeldungen. Nutzername, Passwort und Port in der App prüfen.
- HTTPS Port bindet nicht: die Batch-Datei für die URL-Reservierung einmal als Administrator ausführen, Menü Settings, Network and Security, Register HTTPS port (Admin).

Aktuelle Fassung und Readme: sat-ip-anywhere.com

Fragen an marco.wegehaupt@gmail.com.

* Sinn der Sache war/ist, dass der Client die Videodaten nicht entschlüsseln muss, was den Akku schont. Wer das recherchieren möchte: „Nenne mir potentielle Angriffsmöglichkeiten bei reinem HTTP/TCP Video-Streaming wobei aber bei jedem Connect/ Reconnect ein UUID-Einmal-Token vom Client präsentiert werden muss das vorher per SSL an den Client geschickt wurde. Es geht nur um Live-Streaming (unidirektional), d.h. die Vertraulichkeit ist nicht so wichtig. Wichtig ist aber, dass der Angreifer keinen Zugriff auf den VLC-Transcoder bekommt, was gewährleistet sein sollte, da ein vorgeschalteter TCP-Proxy keinen Zugriff ohne Token zulässt.“